IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

U.S. PATENT APPLICATION

FOR:

LOCATION-BASED CONTENT PROTECTION

INVENTOR:

TIMO VATAJA

Morgan & Finnegan L.L.P.
345 Park Avenue, 22nd Floor
New York, NY 10154-0053
(212) 758-4800 (Telephone)
(212) 751-6849 (Facsimile)

1775 Eye Street, N.W., Suite 400
Washington D.C., 20006
(202) 857-7887 (Telephone)
(202) 857-7929 (Facsimile)

Attorneys For Applicant

LOCATION-BASED CONTENT PROTECTION

BACKGROUND OF THE INVENTION

Field of the Invention:

The invention disclosed broadly relates to methods for providing location-based content protection, and to encoding content with location-based authenticating data for secure distribution.

Background Art:

Multimedia content, such as audio, video and photographic images have become more integrated into data communication. As the number of content distributors increase, the need for content data verification will likewise increase. New technologies and business models will allow greater quantities of multimedia content to be distributed from various locations along data communication lines. As users or purchasers obtain the content, there will be a need to efficiently authenticate the origin of the data and protect the content. Thus, the present invention addresses the need by providing location-based protection for multimedia content or data. By providing an easier model for protecting content, content

creators will have greater security in releasing content, while content users will have confidence that the content is genuine.

SUMMARY OF THE INVENTION:

The present invention discloses a system and method for protecting multimedia content data, such as photographs, video and audio, with location-based data. When a user creates content on a multimedia device, the content is automatically encoded with location-based data. Under an embodiment of the invention, the encoding process is integrated with an electrical switch on the multimedia device (e.g., shutter button). Once the switch is activated, an algorithmic process is executed to encrypt the encoded multimedia content data.

DESCRIPTION OF THE FIGURES:

Figure 1 illustrates a system view of content authentication under an embodiment of the invention;

Figure 2 discloses the transmission of content among the content server and other devices of the present invention;

Figure 3A discloses the creation, encoding and distribution of content with location signatures under an embodiment of the invention;

Figure 3B discloses the creation, encoding and distribution of content with location signatures under another embodiment of the invention;

Figure 4 discloses a method in which protected media is created;

Figure 5 discloses a method in which content is protected through a Content Certification Company (CCC).

Figure 6 discloses an example of media encoding under an embodiment of the present invention.

DISCUSSION OF THE INVENTION:

The invention applies to content-creating devices, such as digital cameras, digital video cameras, digital audio recording devices, and any other devices that allow a user to record visual or audio images, including text and other communicative indicia. These devices may be stand-alone devices, or may be integrated into wireless telephone or PDA devices. **Figure 1** illustrates a system view of content authentication under an embodiment of the invention and how content data is gathered and encrypted. The content data is shown in the format of one or more of the following: photographic pictures **100**, audio **101**, and video **102**. As the content is created alone, or in combination with other content, it is collectively transmitted to the content combination program **106**. Time **103**, location **104**, and device **105** data is also sent to the content combination program **106**. The time **103**, location **104**, and device **105** data may be incorporated as authentication data, provided from trusted sources. The trusted source may be based on identification protocols such as an identified content device and/or user. Under an embodiment of the invention, the identification protocols are automatically embedded into the content metadata (via "one-click" protection, and is shown in greater detail below in **Figures 3A and 3B**. The identification data would include such data as location information and/or data, content creation time, appropriate International Mobile Subscriber Identification (IMSI) and International Mobile Equipment Identification (IMEI) codes. The location data includes Global

Positioning System (GPS) coordinates, as well as coordinates established through such systems as Bluetooth™, IEEE 802.11, Wireless LAN (WLAN), HiperLAN. The location data can also be retrieved from a mobile phone network wherein the location is determined based on one or more cells of the network.

Once the content and authentication data is collected in the content combination program **106,** the system will now have a sample code of the content along with the authentication data. The system then secures the authentication data to the content through content encryption **107**, metadata encryption **108**, and/or a "hash" encryption **109**, each of which is well-known in the art. Once an encrypted signature based on the authentication data **103**, **104**, and **105** is integrated into the content file, the file is then transmitted to a Content Certification Company (CCC) **110**, or other distributor or Rights Management (RM) provider. The integrated signature then identifies the content owner, along with the location and time in which the content was created. Once the provider **110** stores the content, it can subsequently be made available for trusted distribution.

The network may also be formed as a digital wireless wide area network (WAN), based on architectures such as Global System for Mobile Communication (GSM), IS-136 TDMA-based Digital Advanced Mobile Phone Services (DAMPS), Personal Digital Cellular (PDC), IS-95 CDMA-based "cdmaOne" System, General Packet Radio Service (GPRS) and broadband wireless architecture such as W-CDMA and Broadband GPRS. Anoter alternative includes Digital Video Broadcasting, such as DVB-T. DVB-T is related to DVB-C (cable) and DVB-S (satellite), and is the terrestrial variant of the DVB standard and is a wireless

point-to-multipoint data delivery mechanism developed for digital TV broadcasting and based on the MPEG-2 transport stream for the transmission of video and synchronized audio. DVB has the capability of efficiently transmitting large amounts of data over a radio channel to high number of users at a lower cost when compared to data transmission through mobile telecommunication networks using systems such as UMTS/GPRS.

In another embodiment of the invention, **Figure 2** illustrates the transmission of content data among the content server and other devices. **Figure 2** discloses the transmission of multimedia content to content server **203**, which delivers the content to requesting users. The content data is originated from user terminal **200**. The user terminals may be equipped with "one-click" protection (see below in **Figure 3A**) that would automatically encode the content, and further records of user environment data (e.g., location, time, IMEI, IMSI, Memory Card ID etc.) together with the created content. Under the embodiment of **Figure 2**, content from the user terminal is transmitted to content server **203**. The user terminal then makes a request for authentication to operator or authentication provider **202**.

Authentication provider **202** is set up under the embodiment to facilitate verification the authenticity of the created content by sending authenticating data separately to the content server **203**. Once the authentication data is received, content server **203** then links the authentication data to the content created from user terminal **200**. Once encrypted, content server **203** transmits the protected content to remote users or subscribers. The request for authentication may also be

sent to authentication provider **202** via service provider **201**. The content data is processed to prevent or to detect tampering with the content. The content signature (or "hash") can be sent through service provider **201** and then to content server **203** to compare the signature formed there of the received content data. The authentication under the present invention may be accomplished on-line, off-line, or in various combinations. The content and authentication may further be subject to Digital Rights Management (DRM) procedures.

Another embodiment of the present invention is shown in **Figure 3A.** Location data **301** and the date and time **302** are transmitted to multimedia apparatus **303**, and is sent to mobile portion or unit **304**. The location data **301** and the date and time **302** may be generated from external sources (such as a GPS unit), or may be integrated as a single unit into apparatus **303,** with internal location and date/time protocols. Camera **305**, or other multimedia audio/visual (A/V) device, initiates the creation of a multimedia file (e.g., video, audio, etc.) that is subsequently transmitted to media generation portion **306** of apparatus **303**. Media generation portion **306** algorithmically processes the data into a digital media format, such as JPEG, WAV, AVI, MPEG or other similar formats. At the same time the digital media is being formatted, mobile unit **304** prepares location data **301**, date and time data **302**, as well as IMEI, IMSI, Memory Card ID or other similar identification information to be encoded to media generation portion **306**. A user private key **308** may also be transmitted and encoded to the media for additional encryption protection. An encrypting algorithm **309** utilizes the data from media generation portion **306** and then utilizes location data **301**, date and

time data **302**, as well as identification information such as e.g. the IMEI and IMSI information to encrypt all the data collected in the media generation portion **306**. Algorithm **309** may include a "hash" algorithm that is offered by the CCC. Once encrypted, the protected media file **307** is then sent to CCC **310**, where it will be stored and subsequently transferred to a requesting retail site **312**. CCC **313** may also contain user public keys **313** to decode any users keys **308** that are transmitted with the file.

Figure **3B** discloses another embodiment, where the location data **301** and the date and time data **302** are transmitted to multimedia apparatus **303**. Location data **301** and the date and time **302** are then stored in mobile portion **304** of apparatus **303**. Camera **305**, or other multimedia A/V device, provides an initial multimedia file (e.g., video, audio, etc.) that is transmitted to media generation **306** portion of apparatus **303**. At the same time, mobile unit **304** transfers location data **301**, data and time data **302**, as well as identification information such as e.g. IMEI and IMSI information to media generation portion **306**. Encryption algorithm **309** is provided to encrypt the information stored in the mobile portion **304**, and may be further integrated into a Public Key Infrastructure (PKI) system. Through PKI, user public keys can be managed on a secure basis for distribution systems (e.g., IETF X.509 standard). Once protected media **307** is established, it is forwarded to CCC **310**. CCC **310** may also be configured to store public keys **313** of registered users, wherein location signatures **311** are affixed to the media files prior to being sent to any retail sites **312**. Location signature **311** would typically include such data as location, date, time, user IMSI and IMEI and file size. Location signature

311 would then electronically "watermark" the content to prevent tampering. It is understood that the public/private key arrangements may be implemented in various ways and combinations under the disclosure of the present invention to allow the encryption/decryption of data.

Turning to **Figure 4**, the encryption of the media content begins with the initialization of content creation **400**. The initialization can occur through the activation of an electrical switch, such as that found on a camera shutter-release, or other media device. If creation of the media has not been initialized, the process waits **406** until content creation has been initialized. Once initiated, the process proceeds to **401**, to determine whether Location Based Content Protection (LBCP) is active. If it is not activated, an unprotected media file is created **402**. Under alternate embodiments, the LBCP may be automatically integrated into the media device, so that LBCP may be permanently set to an active state. Once the LBCP is set, the process proceeds to request user location signature data **403**. Once received, the process runs encryption algorithm **404** to append the location signature data to the media file. Depending on the environment used, the location signature data may be embedded into the file, or may be attached to the file metadata prior to further transmission. Once signature data is encoded, media file is released as a protected media file **405**.

Another embodiment is disclosed in **Figure 5**, where a new media file is created in user device **500**. Once created, the device automatically records user location signature for created content **501**. A signature preferably contains such information as the date and time the content was created, as well as the user

location. Furthermore, the user's device will typically possess IMSI and/or IMEI capabilities. Once a signature is established, the process moves to **502**, where media content characteristic data (e.g., type of file, size of file, etc.) are rendered. The content characteristics may be further associated associated with the location signature. The media content, content characteristic data and location signature are then transmitted to CCC **503**. Under the embodiment of **Figure 5**, media and location signature/media characteristic data are sent separately to a CCC. A CCC may be set up so that each user sending multimedia data must be pre-registered as a subscriber. Under this embodiment, the CCC confirm's the user as a subscriber **504**, either through a password, or through automatic identification of the user's IMEI/IMSI. The CCC would then run encoding algorithm **505** to protect the content under a location-based content protection (LBCP) protocol. Once encoded, the protected media would be ready for secure transmission and distribution to requesting users.

One example of media encoding is given in **Figure 6**. In this example the metadata file **601** comprises, in addition to the location signature data such as location, date, time, device and/or user identifying data and file size, also a "hash" signature of content file **600**. In the example, the "hash" signature is shown as "acek321idksl", which is created by using an "hash" algorithm. The "hash" signature can be used for detecting any tampering with the content. The "hash" algorithm can be selected from a plurality of algorithms available on the mobile device. An ID for the selected algorithm can be included in the metadata of the content file. The CCC can identify the used algorithm based on the ID and can run

a check for identifying any tampering on the content file. In another embodiment of the invention the "hash" algorithm can be applied to the metadata associated with the content and his "hash" is sent to the CCC.

The utilization of location-based protection provides an additional level of verification to media files, and provides additional protection against unauthenticated distribution of digital rights. Under the present invention, if a third party attempts to scan a verified picture, no location data is copied into the file, and the CCC would not accept the file. Also, the CCC could be configured to accept only certified user apparatus and application data, so that fraudulent location/content combinations would not be accepted. CCC's and mobile operators may also make arrangements to have IMEI verification of user locations.

There are a multitude of applications in which the present invention may be used. Content sites can provide a wide spectrum of location based content, from wildlife pictures to news reporting and entertainment. Insurance companies could set up servers where users could effectively transfer protected accident photographs. Police photographs could incorporate the invention to validate photographs taken at traffic intersections or speed traps. The present invention can also be used for reporting of progress in construction or assembling projects. Various games based on "scavenger hunts" could incorporate the technology to create revenue generating or promotional activities for businesses.

An alternate application of the invention the content is delivered through the content server with authentication data to broadcasted programs as a part of the broadcasted program or inserted to e.g. advertisements which are sent in

broadcasted transmissions. The authenticated content can be delivered even in real-time.

An alternate application of the invention includes the content-creation devices as being connected to or integrated into mobile communications devices. This way, the devices can be remote-controlled by the user to be used e.g. for monitoring purposes. Still another application of the invention includes a content server for distributing or transmitting the authenticated content to other terminals. The authenticated content can in one embodiment of the invention also be sent to other terminals connected to the network e.g. as a multimedia message such as MMS or other similar message.

Although illustrative embodiments have been described herein in detail, it should be noted and understood that the descriptions and drawings have been provided for purposes of illustration only and that other variations both in form and detail can be made thereupon without departing from the spirit and scope of the invention. The terms and expressions have been used as terms of description and not terms of limitation. There is no limitation to use the terms or expressions to exclude any equivalents of features shown and described or portions thereof.